#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Andrew Charles David Hay, et al.) Group: 2152

Serial No.: 09/931,657) Examiner: not yet assigned

Filed: August 16, 2001) Our Ref: B-4271 618992-5

For: "SECURITY APPARATUS") Date: November 20, 2001

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231

Attn: Customer Service Center
Initial Patent Examination Division

Sir:

[X] Applicants hereby make a right of priority claim under 35 U.S.C. 119 for the benefit of the filing date(s) of the following corresponding foreign application(s):

COUNTRY	FILING DATE	SERIAL NUMBER
Great Britain	18 August 2000	0020438.8

[ ] A certified copy of each of the above-noted patent applications was filed with the Parent Application No._____.

[X] To support applicants' claim, certified copies of the above-identified foreign patent applications are enclosed herewith.

[ ] The priority document will be forwarded to the Patent Office when required or prior to issuance.

Respectfully submitted,

Ross A. Schmitt

Ross A. Schmitt
Attorney for Applicant
Reg. No. 42,529
LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300
Telefax: (323) 934-0202

U N 09/931,657

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 14 August 2001

Patents Form 1/77

Patents Act 1977

THE PATENT OFFICE
18 AUG 2000
RECEIVED

The Patent Office

21AUG00 E562138-1 D01463
P01/7700 0.00-0020438.8

1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 30006646 GB

2. Patent application number *(The Patent Office will fill in this part)* — 18 AUG 2000 — **0020438.8**

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number *(if you know it)* — 00496588004

If the applicant is a corporate body, give the country/state of its incorporation — Delaware, USA

4. Title of the invention — Security Apparatus

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Christopher John Harrison
Hewlett-Packard Ltd, IP Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ

Patents ADP number *(if you know it)* — 07963713001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	26
Claim(s)	1
Abstract	1
Drawing(s)	

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	Fee Sheet

11. I/We request the grant of a patent on the basis of this application.

Signature Richard A Lawrence Date 18/08/00

12. Name and daytime telephone number of person to contact in the United Kingdom: Janet Smith, 0117-312-8026

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

SECURITY APPARATUS

Background Art

A modern computing apparatus includes many different components (the word "component" is used here to describe essentially any discrete functional element of a computing platform, including either a piece of hardware, a piece of software or a piece of firmware), most of which are standardised and can be upgraded.

Computer-based training is an interactive technique used for training computer users on a number of software applications. Its success lies in the fact that the instructional method uses the actual end-user software to illustrate and demonstrate proposed tasks and procedures. Computer based training tends to be a one-off educational affair, designed to achieve an eventual level of expertise. The Interactive Instructional Feedback Assistant within this invention uses the same concept, but as a method for teaching, the Interactive Instructional Feedback Assistant is incremental at instructing on particular tasks, rather than requiring the user to spend a large amount of time completing full instruction on the whole system. In HCI terms, this distributes the costs of implementing the security features over time, making the use of such features more likely. Also, the fact that all possible security functions provided by the Trusted Platform Hardware will be presented to the user when relevant, on a level which is relevant to them, means that all functions are likely to be viewed and employed at some time or other when required, rather than the user having to spend time setting up all features before using any, or having to search out required features. This will reduce the amount of functions that are not used because they are not found

In addition, Human-Computer-Interaction emphasises the need to reduce the costs to users to a minimum when engaging in any task, so that the benefits

of that task make the costs worthwhile. The Interface Assistant described in this invention is based on this concept by modelling the system behaviour in a way which is relevant both to the user and to the tasks a user may wish to carry out, while ensuring that the costs to the user (from lost time, etc) are kept to a minimum in relation to the benefits which the added security can give, and can be conveyed to the user. The Interface Assistant represents to users a model of the system structure and system behaviour that is relevant and simple. By doing this, the user feels involved in the security of their computer at a level at which can feel competent.

The psychological component of Human-Computer-Interaction describes the way people 'think' about machines and their functions. People have 'schemas' or 'mental models', which are their own simplified framework models of a system that allows the user to store knowledge about the system (Schemas and mental models are general cognitive psychology concepts). Because computers are very complex systems, the process of a person developing an adequate 'mental model' of computer security from their very limited (and very high-level) experience of computer security, is very unlikely. Undeveloped models are fragmented and do not allow people to make trustworthy predictions from them, which is a possible reason people do not actively engage in using or seeking out computer security - the costs (due to the complexity) are perceived to be too high.

Construction of a simple model of a computer and its major components creates a ready-made framework for users that is complete and comprehensible. With a framework model of the computer system to refer to, simple representations of computer behaviour can easily be conveyed to users. With a relevant framework available to users, and an understanding of computer behaviour in relation to that framework, then users can be shown aspects of the computer behaviour which may be made more secure (in terms

of the model). Thus, security and privacy risks can be represented to users in terms of the simple system model, which allows a high-level understanding of the computer's security issues to be developed, alongside a high-level understanding of security tools, which is 'relevant' to the users. Users are given a complete understanding of the system from the system model, from a high-level, which compares to a previously untrusted and incomplete model of system behaviour that may have existed on many levels. A trusted model leads to trustworthy predictions which allows the user to feel confident about having a high-level control of the system security, with maybe some help and instruction from an assistant to the model that fills in knowledge gaps, and shores-up the model.

Trust in the context of networked communication will be composed of factors such as the ability for a user of a computer system to feel confident that they know who and what they are talking to, that the communication is confidential and that the information is transmitted accurately. In a world where software attacks are not uncommon, this trust cannot be taken for granted and needs to be based upon technological mechanisms. Many security-related mechanisms are or will shortly be available, and each can enable certain types of communication or information to be trusted to differing degrees.

For example, in order to build a trusted relationship between the computing apparatus and its users, a recent solution has been proposed [application ref. 30990050 Trusted Platform], namely platform integrity checking. With this solution, the computing apparatus has a physical located trusted device, which is used to make trusted measurement and trusted reporting for each functional component. This solution allows devices to challenge the trusted device in order to check integrity of one particular component. Then, the trusted device will respond to the challenge by sending a signed report of this functional component. The report tells the challenging device related

information about the component, such as the model of the component, manufacturer of the component, version of the component, upgraded data and so on. After receiving the response, the challenger will make its own decision whether or not to trust this particular component, and furthermore after checking a number of selected functional components, the challenger will make a decision whether or nor to trust the computing apparatus.

One useful feature, which has not been covered by these prior art solutions, is how the user of the computing apparatus is able via a user interface to appreciate or better understand security mechanisms such as platform integrity checking, different types of platform identity that can be trusted to varying degrees, more and less protected forms of storage, hardware versus software-based security, cryptographic functionality, and so on, and further to be able to use such information to select the most appropriate solution in order to try to ensure that the communication or computer-based action in which the user engages can be trusted (that is to say that it always behaves in the expected manner for the intended purpose).

Users of computing apparatus will appreciate having a software interface which explains to them how to use computing apparatus hardware or security features associated with that hardware. The need to convey the functionality of trusted computing apparatus in relation to existing hardware structures within the computing apparatus, in a simplified way, is of paramount importance to both vendors and purchasers of hardware that increases trust in computing apparatus. Having an interface assistant that explains and teaches users about the risks that trusted computing apparatus is designed to combat, will ensure users that better employ the available services provided by such apparatus.

Summary of the Invention

In accordance with a first aspect of the present invention there is provided a security apparatus comprising a receiver for receiving a security metric associated with a computer entity; means for presenting to a user the security metric; means for modifying a security setting associated with the computer entity to enable the modification of the security metric associated with the computer entity.

Preferably the security metric is presented to a user as a representational model of software and/or hardware functionality of the computer entity.

Preferably the security apparatus further comprising input means for allowing a user to interact with the modifying means to modify the security setting.

Preferably the security apparatus further comprising means for establishing possible modifications to the security setting based upon the received security metric.

Preferably the level of complexity of the presented is selectable by a user.

In accordance with a second aspect of the present invention there is provided a method for modifying the security status of a computer apparatus, the method comprising receiving a security metric associated with a computer entity; presenting to a user the security metric; modifying a security setting associated with the computer entity to enable the modification of the security metric associated with the computer entity.

The invention is an interface assistant that explains and teaches users about the risks that computing apparatus is designed to combat so that users

understand and/or can better employ the available trust-enhancing features and services provided by the platform. This interface assistant is a software user interface that uses an internal real time representational model of software and hardware functionality to represent security risks to the user, to highlight or explain trust- or privacy-enhancing features of the platform, to display security choices related to the user's current or next desired action and/or to allow the user to configure security settings.

The interface assistant is software to enable users to understand and make choices about trusted mechanisms on their computing apparatus by means of an interactive instructional feedback 'assistant' which represents to the user certain security risks in a simplified fashion.

Preferably the interface assistant is modelled on a 'real-time' representational model of software and hardware functionality that acts as an important source of feedback to the user, and all functionality is through the same "porthole" of the interface, which is the system model.

Preferably, the interface assistant also includes a trusted platform hardware control that acts as the functional component of the interface assistant and allows the user to define trusted platform security settings, as well as control software and hardware within the computer in a way that may increase computer security. This trusted platform hardware control will take a similar form to the interactive instructional feedback assistant, but its functionality will depend on what mechanisms for increasing platform security exist in the corresponding computing apparatus. Preferably, these security settings are protected from being altered by an unauthorised entity.

Optionally, the trusted platform Hardware Control allows users to request certain metrics from any trusted computing apparatus which are reported back

to the user via the user interface, by using the integrity reporting mechanism of the prior patent described above.

Optionally, the trusted Hardware Control allows the user to isolate or quarantine files,folders,programs or even hardware devices by selecting the representation of these objects within the trusted hardware control and then requesting the OS to place these devices within different compartments within the computer apparatus.

Preferably, a history of the user's cancelled tasks when using the interactive instructional feedback 'assistant' may be saved for future reference by storing such tasks in a short-term memory store within the computing apparatus.

Optionally, the invention provides a method of establishing a security configuration database by listing the user's chosen security-related configuration of functional components and related information

Optionally, the invention provides a method of protecting this configuration list in a secure manner if required by using either a trusted token of the user or the protected storage of the computing apparatus.

Optionally, the invention provides a method of protecting this interface assistant in a secure manner by using an extension of the method of prior art to take an integrity measurement on the interface assistant as part of a trusted boot process or platform integrity check. By these means a challenger would be able to detect if the interface assistant had been altered in an unauthorised manner.

Description of the Preferred Embodiment

The embodiment of a trusted platform is as described in patent application [ref. 30990050 Trusted Platform], and has as its central feature the incorporation into a computing platform of a physical trusted device whose function is to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform. The identity and the integrity metric are compared with expected values provided by a trusted party (TP) that is prepared to vouch for the trustworthiness of the platform. If there is a match, the implication is that at least part of the platform is operating correctly, depending on the scope of the integrity metric.

1) The system model

The system model is a 'reduced' model of a computer that includes the hardware and software. The model is designed to represent to the user a high-level overview of a computer, which can allow high-level security functions to be carried out. Lower-level functionality is possible through 'drilling down' through the high-level model into a progressively more representational model of the computer platform and its components.

The System Model is the primary on-screen component. This is always present either full-time in such a way that it does not obscure users from their primary tasks, or it will appear whenever the system performs some action (which shall then be represented to the user). This component is an essential requirement for familiarising the user with the system behaviour in terms of the System Model. Every function carried out by the system will be translated to the user 'real-time', so that the user is aware of that function in terms of the System Model. All hardware and software will be mapped by the Trusted Platform Hardware so that any hardware or software which requires system resources can be determined by the Trusted Platform Hardware (if this is possible) The user will not have to respond to the System Model to cancel or

to OK the 'real-time' representations of the System Model (this real-time System Model will work in a similar way to the computer's 'Task Manager'); these will carry on simultaneously until interrupted by the user, or by the Interactive Instructional feedback Assistant.

The user may interrupt the System model in order to request further information about some aspect of the system behaviour reported via the System Model by dragging the mouse over the System model, which will immediately reveal the Trusted Platform Hardware Control. If the user does not click on the Trusted Platform hardware Control, the System Model will return to view when the mouse is dragged off the display.

The Interactive Instructional Feedback Assistant will interrupt the System Model to emphasise any system behaviour which could be made more secure, via the Trusted Platform Hardware Control. This is carried outy checking the configuration of software and hardware with relation to the available security functions in the Trusted Platform Hardware Control and the task being undertaken by the user (either all in relation to each other, or simply one against the other as in encryption, where sending a file will trigger feedback if the file has not been encrypted with the Trusted Platform Hardware Control) the Trusted Platform Apparatus can determine what suggested tasks can be presented to the user.

The importance of the System model is to familiarise the user with the way system behaviour is represented throughout the device, and also to make the user more aware of system behaviour, and the behaviour of the Trusted Platform Hardware in relation to the System behaviour. The user shall be able to review all these occasions if they wish, through the Trusted Platform Hardware control.

2) Interactive Instructional Feedback Assistant

The interactive Instructional Assistant, or Security Assistant, represents relevant security concerns to the user in terms of the high-level system model. This assistant recommends tasks to the user, in order to increase the security of the computer platform. If the user is unsure of the security risk, or the security issue, they are able to progress through a simplified explanation of the security issues and the task based on the system model [e.g. by following on-screen prompts which guide the user through a short explanatory screen sequence explaining the task]. This instructional assistant allows users to drill down for further information about the task, or about the components of the system that may be affected by the task. The instructional Assistant emphasises the way that security is derived from the trusted platform hardware, and how the trusted platform hardware contributes to the separate security tasks recommended by the security assistant.

The Interactive Instructional Feedback Assistant will represent to the user an 'at risk' component (whether software or hardware). This representation must take on the form of the System Model, or a simple representation derived from the system model, which the user shall be familiar with. Along with the representation, a proposed task shall be presented to the user which will increase the security of the 'at-risk' component and/or other related components. If the user accepts the proposed task, they will go straight to the Trusted Platform Hardware control, which shall allow them to perform the suggested task. If the user wants more information about the nature of the risk and the proposed solution, the Interactive Instructional Feedback Assistant will take the user through a high-level description of the risk and the solution, and the major components and/or processes involved. These high-level descriptions incorporate diagrams derived from the System Model and text accompaniments. Users are able to click through the screens and then get the

choice to follow through with the originally proposed security task, or just cancel.

Preferably, a history of cancelled tasks may be saved in a short-term memory store within the Trusted Platform Apparatus for users to come back to.

Each screen also allows the user to drill for further information about the components represented to them on the screens, and then return back to the original screen. Preferably, all actions can be cancelled, and all screens are navigable in a similar manner and using similar mechanisms to an Internet browser i.e. users are able to go forward/back individual screens, or jump screens, whilst always being able to find their way back to where they began.

Preferably, users are able to configure the Instructional Assistant to determine whether the Assistant will interrupt the user if there is a potential security risk, or whether the Assistant will attempt to grab the user's attention without interrupting their task. This can be achieved by selecting the appropriate option in a 'SET-UP' screen which is accessed by clicking on Set-up in the Trusted Platform Hardware Control Menu screens...

3) The trusted platform Hardware Control

The trusted platform Hardware Control is the functional component of the interface.

The trusted platform Hardware Control is the functional component of the interface. This control is accessed either from the Instructional assistant (when it interrupts the user signifying a potential security risk), or through the Real-time representational model of the system (which is preferably constantly present on the desktop), or available to call-up at anytime through a short-cut

key or via an icon in the start-up menu. The control allows the user to select a security function from a component specific menu (i.e. Hard-Drive, Inputs/Outputs, File, Program, etc), by clicking on a component icon/button upon the system model. For example, clicking on the Hard Drive icon may suggest virus scanning, integrity checking, File management, etc., specific to the Hard Drive. Alternatively, clicking on the Output icon/button would give a list of output components (Disk Drive, Modem, etc). If one were to select the modem, then virus scanning may not be a relevant option, whereas intrusion detection would be. This is what is meant by 'context specific'.

Preferably, if at any time during using the Trusted Platform Hardware Control the user requires further information, the user can request the context dependent Interactive Instructional Feedback Assistant to represent to them the relevance of the functions contained within the control, in relation to the system model and the system behaviour, or the current risks associated with the component configuration and the expected gains from the suggested changes to the component configuration. This can be done by clicking on the Interactive Instructional Feedback Assistant Icon which will provide help for any highlighted topic on one of three levels (LOW/MEDIUM/HIGH complexity – selected from a button from within the screen opened by the Interactive Instructional feedback Assistant Button). The Trusted Platform Hardware Control will represent possible functions to the user in one of a number of ways. The users will have a System Model with which they can click and select components they wish to examine, configure, and set-up according to the services provided by the Trusted Platform Hardware. The user will be given the option to use major security functions from the outset i.e. encryption, virus scanning, integrity checking, etc., which will be available through clicking onto anicon (for example, a Trusted Platform icon).

Optionally, there is also a second form of accessing functions, which is a general security menu suggesting functions such as Integrity Checking of the computer platform via the trusted platform Hardware. This option would be presented to the user as an alternative to the above option, and would be accessed from the first option screen, by clicking on a menu button, and then the Security functions button. Users would be able to scroll through Security functions, and get a brief description of each of those functions, and options relevant to those functions (e.g. Virus scanning will give options to scan messages in mail, to scan disks, or configure the scanner, etc). They can also choose to get the Interactive Instructional Feedback Assistant to take them through the function by clicking on the relevant icon when the function is highlighted.

The user is able to specify a secure configuration for the entire computer or individual components on three different levels (LOW/MEDIUM/HIGH – complexity) requiring different knowledge levels. This service would be available through either of the main Trusted Platform Hardware Control menus. The trusted platform Hardware Control allows the user to refer back to the instructional device if they had a difficulty configuring the trusted platform Control (an icon for the Interactive Instructional Feedback Assistant will be present on all screen to help with all major functions). Any changes made to the trusted platform control would be reversible, with all previous configurations saved according to date and time of the configuration change, and accessible through the function menu. These saved configurations can be reinstated at any time up to a point, when the configurations shall be deleted from a short-term memory store.

The Trusted Platform Hardware Control allows the full functionality of the platform to be explored and configured from a number of levels via the Trusted Platform Hardware Control Menus, and by specifying the complexity

level of functions through clicking on the HIGH/MEDIUM/LOW icon. (see figure 4b). A hierarchical distinction between functions shall be made based on necessary expertise required (LOW/MEDIUM/HIGH complexity).

Preferably the Trusted Platform Hardware Control will allow users to configure individual security components and global security set-ups [for example, by the trusted platform hardware control sending commands to the OS or by storing such configurations in a file that is accessed by software specialised to carry out such configuration]. Essential to the Platform security is the user's capacity to be able to request the platform to configure non-trusted platform components including software (such as Internet Explorer, WORD, etc) and hardware (such as Network connections) to run in a secure way (either suggested by the Trusted Platform Hardware Control or by the user, who can access these controls through the Standard Trusted Platform Hardware Control Menus). These would be secure default setting stored in the TPHC, with the user preferably getting feedback about what the functional implications of the default setting may be.

Optionally, all changes to configurations shall be filed so that a test period can be undertaken under the new configuration. In this case the user will be allowed to return to the original configuration within a set time if the new configuration is not acceptable to their requirements. The set time for returning to an original configuration is determined by the short-term memory storage of the original configuration metrics.

The Trusted Platform Hardware Control allows users to request certain metrics from their computer platform (by means of the. (such as which users had accessed the machine and when, or what changes had occurred to the machine since some set period of time, or some other mark – such as the last time a specific user had used the machine), which shall be reported back to

the user in the form of the user's choice e.g. as a report on start-up, or stored and available if requested. This is achieved using the integrity reporting mechanism of the prior patent described above.

Preferably, the Trusted Platform Hardware Control will allow the user to isolate or quarantine files/folder/programs or even hardware devices, in order to further increase the security of the computer platform under certain high-security conditions, or to reduce the potential of harm befalling these components during 'high-risk' exercises (e.g. downloading a suspect file or program, etc). This can be achieved by using compartmentalisation within the computer apparatus.

Other components' configuration tasks can be obtained by clicking on the relevant component icon and then searching for a specific component to configure, or by applying global configurations to a class of components. At all stages the user may refer to the Interactive Instructional Feedback Assistant for advice or explanations.

Brief Description of the Drawings

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, of which:

Figure 1 is a diagram that illustrates the appearance of the System Model, showing how the computer system has been reduced to six major components, which can all be controlled by the Trusted Platform Hardware. Very simple interactions between these components can be represented to the user.

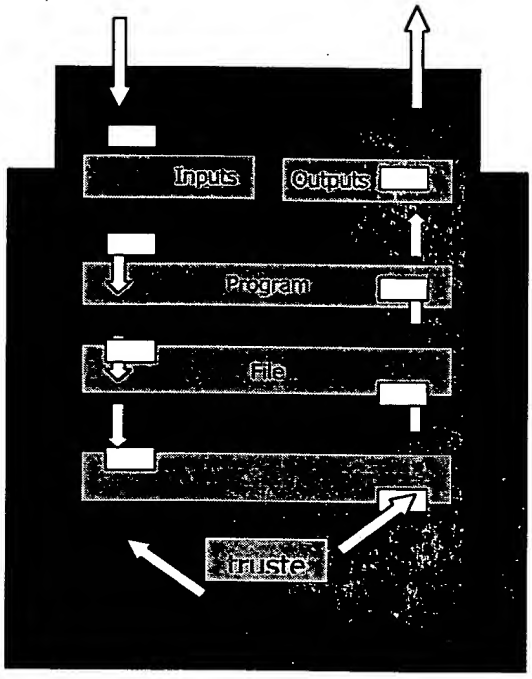

Inputs
Outputs
Program
File
Intruder

Figure 2 is a diagram that illustrates...the way the real-time System Model represents the system behaviour to the user, by highlighting the components involved in the particular system task, and the relationship between those components.

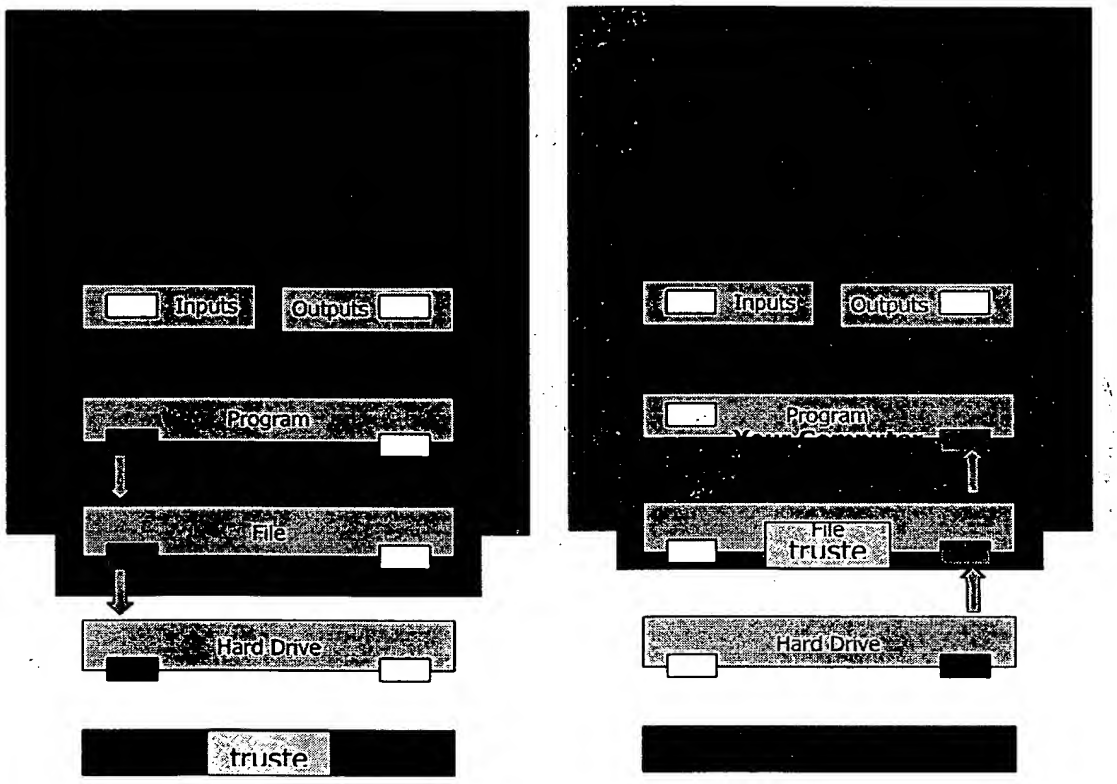


Figure 3 is a diagram that illustrates the way the Interactive Instructional Feedback Assistant presents a risk to the user, and suggests a possible solution.

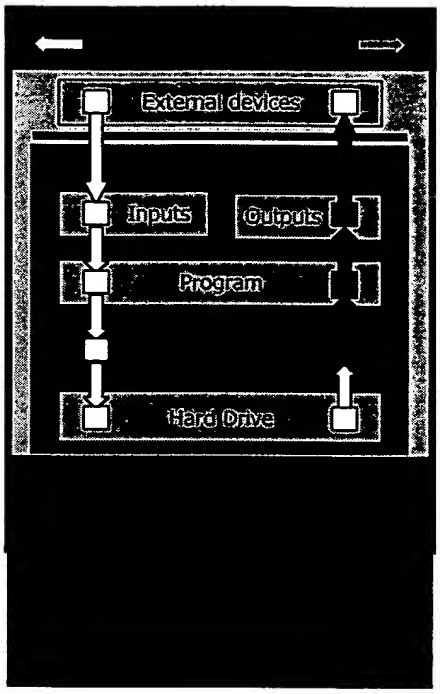
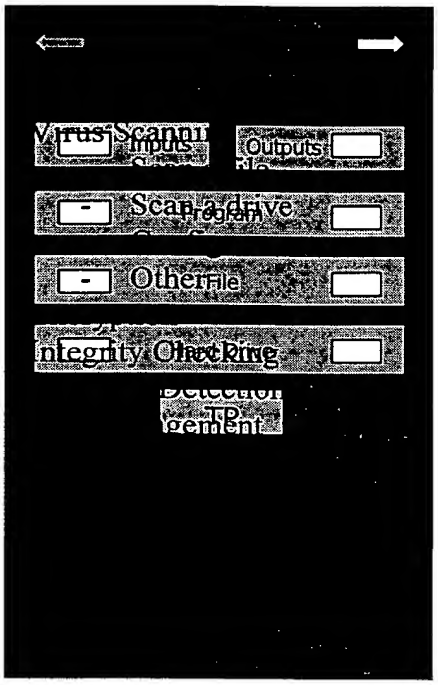


Figure 4 is a diagram that illustrates two of the menu choices in the Trusted Platform Hardware Control, showing the System Model menu in diagram a., and the Function menu in Diagram b. Also shown in diagram b. alongside the virus scanning option is the Complexity Level setting, which differentiates LOW/MEDIUM/HIGH complexity information regarding separate functions (currently set at LOW).

a. b.

Interface assistant

20



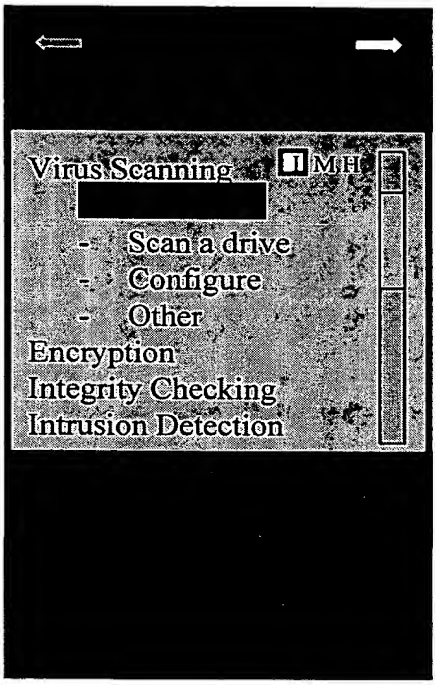
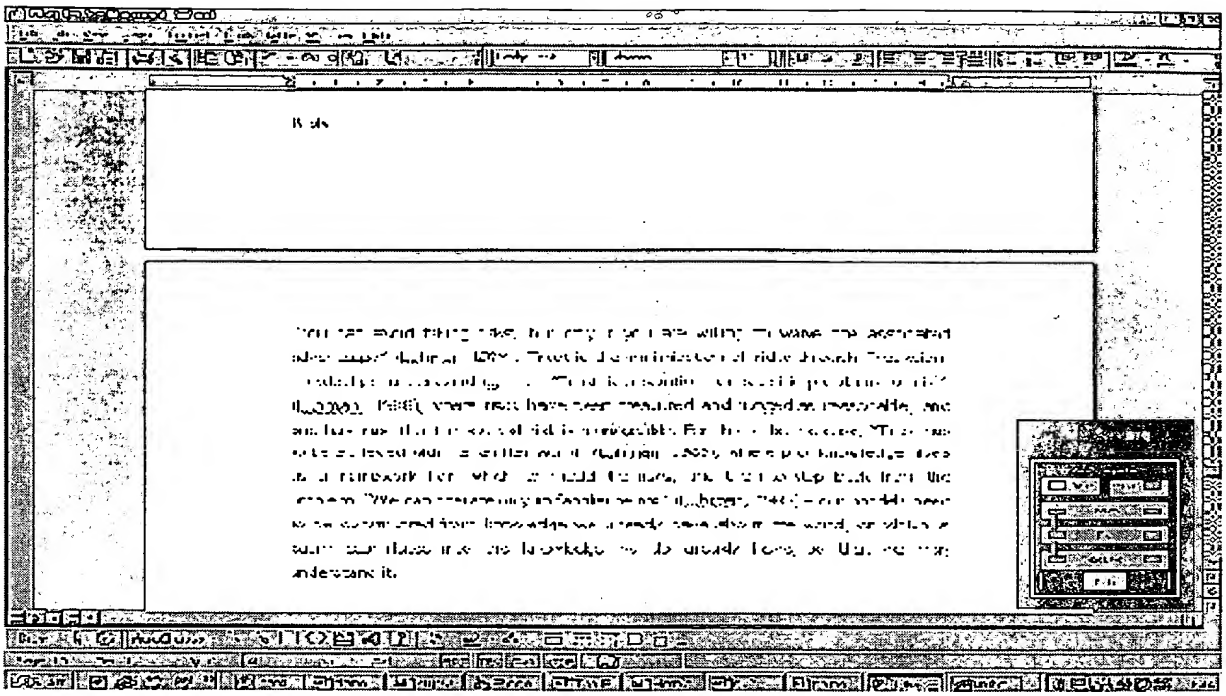


Figure 5 is a diagram that represents the relative size of the real-time System Model in relation to screen area.



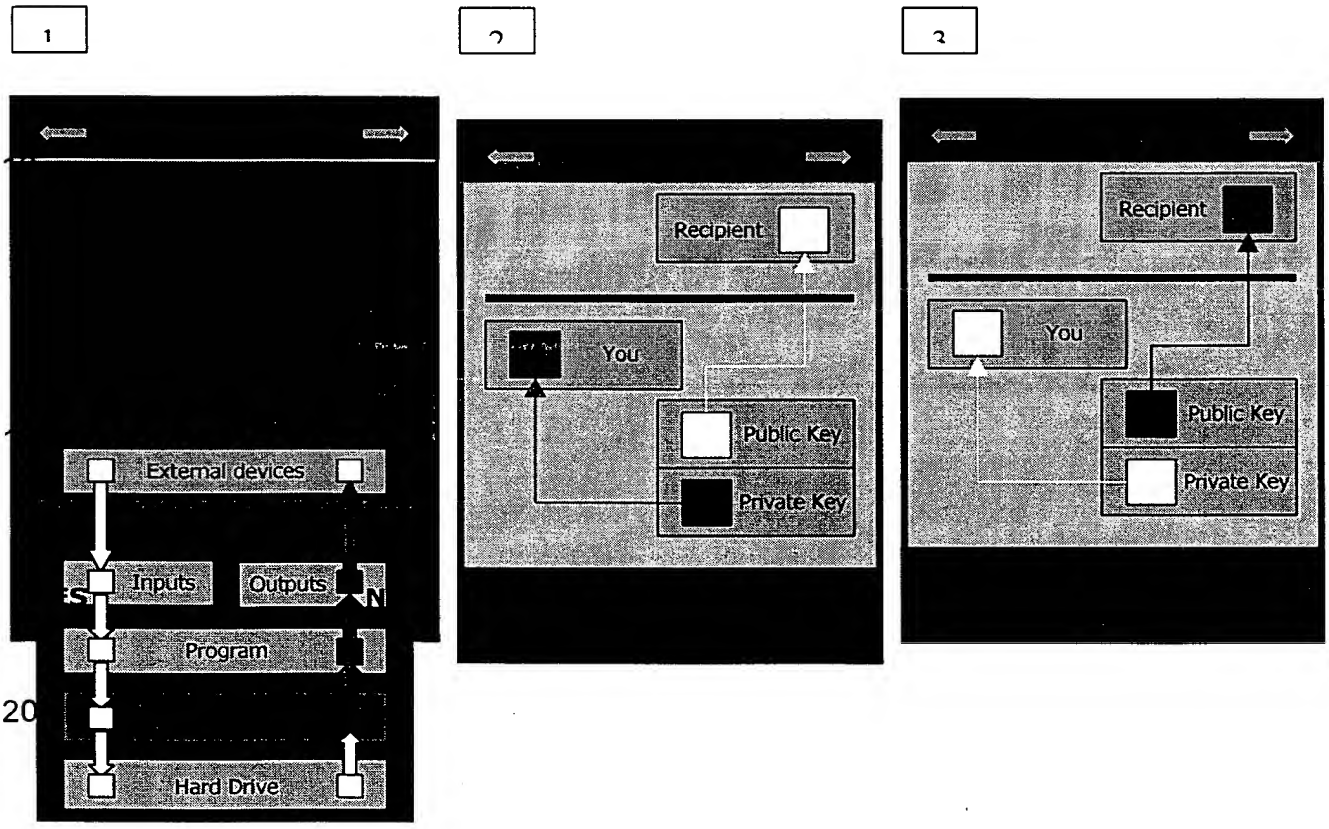
1) *Real-time Representational model of Software and Hardware Functionality*

The system model will form the central focus of the representational model of real-time happenings within the Computer Platform. The system model shall respond to automatic functions that normally happen unnoticed by the user (e.g. Cookie file downloads, autosave/autorecover), as well as those functions which are related back to the user (such as opening a program or saving a file). By giving real-time feedback via the model, users shall quickly get to know and understand the working of the computer in terms of the system model, even if they don't consciously attend to it.

2) *The Interactive Instructional Feedback Assistant* represents a subset of services that are provided or supported by the computing apparatus upon which the assistant is mounted. Possible tasks and instructions include

encryption, virus checking, file management (Cookie files, temporary files, etc), Application configuration (to a more secure configuration), Intrusion detection, file download, Internet transactions, etc.

A possible representation of file encryption using the proposed system model in Figure 3 would look as follows:

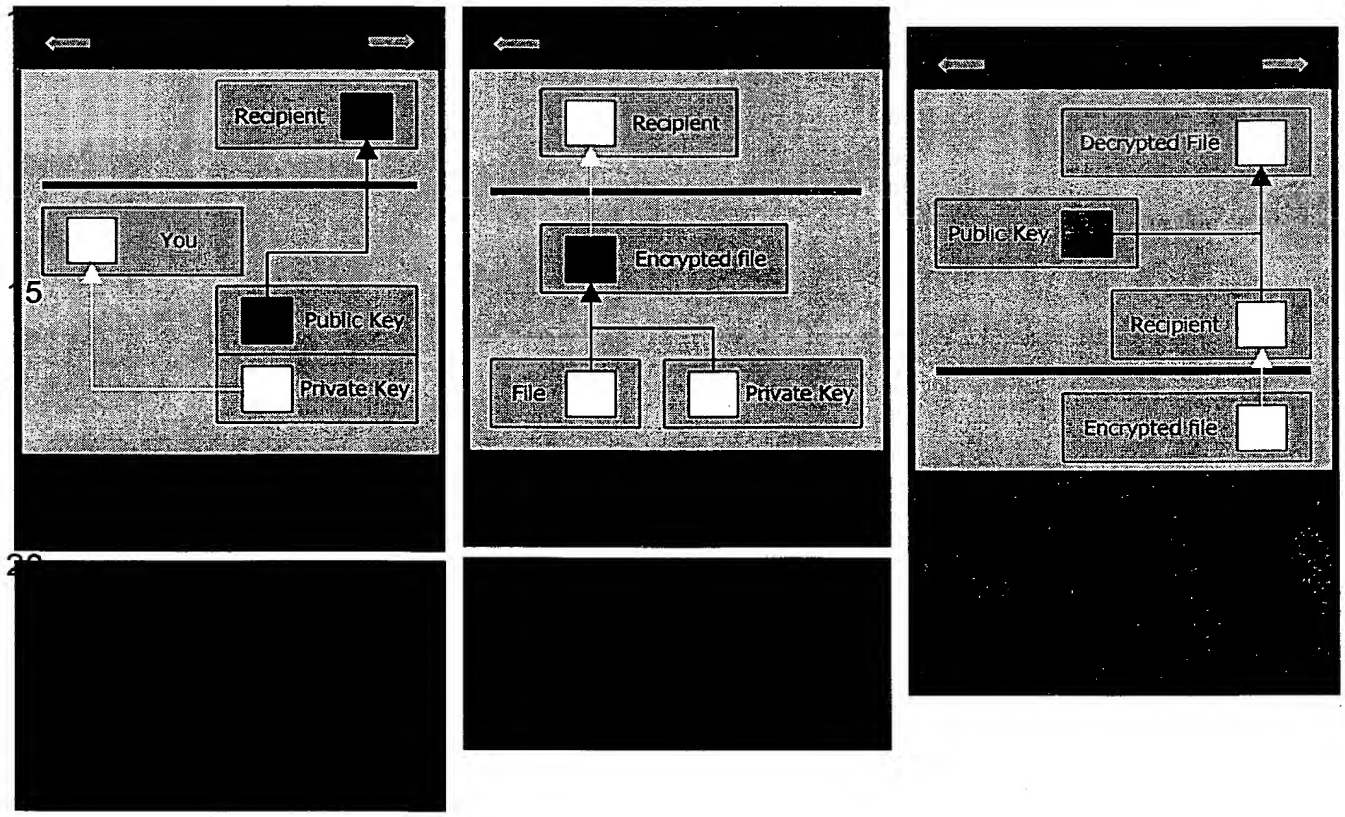


Interface assistant

23

4 5 6

5

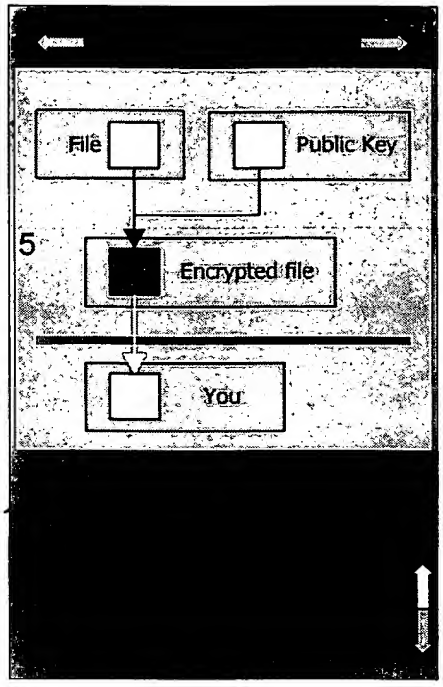


15

20

25

7

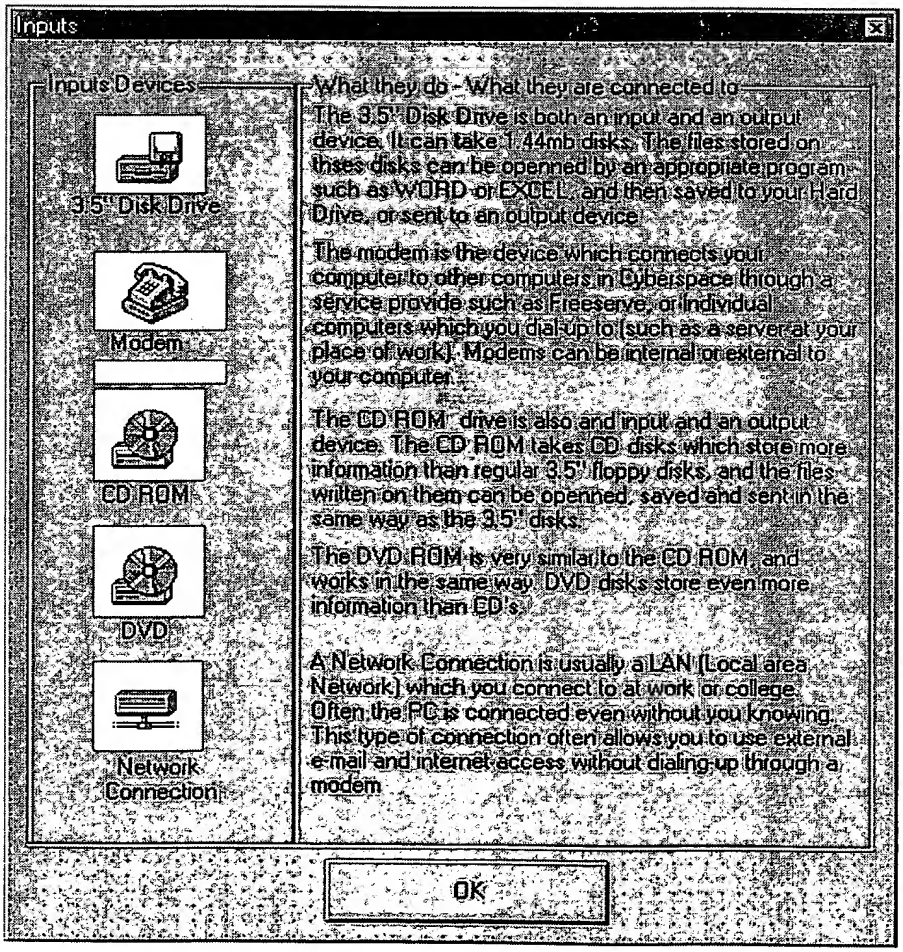


The representation of the process of encryption is preferably at a high level, and directly related to the system model. Lower-level information can be found by clicking-down through the separate screens, revealing greater depths of information on an ever-more technical level, represented to the user via the LOW/MEDIUM/HIGH complexity icons. This enables users to advance their technical knowledge through the interface.

All immediate information is presented to the user at a high-level. Once the user gets familiar with the task presented to them, they can begin to view lower-level instructions without having to drill through the high-level instructions – this is a configuration they are able to determine. This is achieved by setting a control which reveals more functions and further descriptions to the user, in ever more technical language as is necessary for the description. The control for this function takes on the form of a LOW/MEDIUM/HIGH setting, which can be changed at any time during any task. The result of this change would be that each high-level screen (LOW complexity) would be substituted for a more technical representation of the task, depending on the setting. The more technical screens would be directly analogous to the high-level screens and functions, enabling

direct comparisons and references to be made, which would further increase knowledge transfer and learning Preferably, users can go straight to the proposed task screens, which in the case of encryption, would allow the user to go straight to the process of file encryption.

The type of information available by drilling down through the Inputs icon on screen #1, is information about input device types such as modems and disk drives (see below).



A similar screen would also represent available output devices (which often serve a s both input and output devices). The above information screen would be marked as LOW/MEDIUM/HIGH complexity so that users may determine whether they need this information to carry out the task presented to them. It would be possible to click on the icons represented on these screens for relevant but more complex information on the proposed encryption task.

CLAIMS

1. Security apparatus comprising a receiver for receiving a security metric associated with a computer entity; means for presenting to a user the security metric; means for modifying a security setting associated with the computer entity to enable the modification of the security metric associated with the computer entity.

2. Security apparatus according to claim 1, wherein the security metric is presented to a user as a representational model of software and/or hardware functionality of the computer entity.

3. Security apparatus according to claim1, further comprising input means for allowing a user to interact with the modifying means to modify the security setting.

4. Security apparatus according to claim 1, further comprising means for establishing possible modifications to the security setting based upon the received security metric.

5. Security apparatus according to claim 1, wherein the level of complexity of the presented is selectable by a user.

6. Method for modifying the security status of a computer apparatus, the method comprising receiving a security metric associated with a computer entity; presenting to a user the security metric; modifying a security setting associated with the computer entity to enable the modification of the security metric associated with the computer entity.

ABSTRACT

Security Apparatus

Security apparatus comprising a receiver for receiving a security metric associated with a computer entity; means for presenting to a user the security metric; means for modifying a security setting associated with the computer entity to enable the modification of the security metric associated with the computer entity.